VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO - INFO - VIGIDEL INFO - VIGIDEL INFO - VIGIDEL INFO

Mesdames et Messieurs,

Compte tenu de la méfiance des internautes face au phishing, les cyberfraudeurs s'attaquent maintenant à des victimes par l'entremise du vishing.Le vishing, ou hameçonnage vocal, est l'utilisation de la technologie VoIP (voix sur IP) dans le but de duper quelqu'un en lui faisant divulguer des informations personnelles et/ou financières.

Manière d'opérer des fraudeurs :

Première méthode:

Un automate téléphonique est utilisé pour contacter les victimes potentielles en composant au hasard des numéros de téléphone fixe.

Lorsque la victime potentielle décroche, un message pré-enregistré supposé provenir de sa banque la prévient que des opérations inhabituelles ont été effectuées sur son compte bancaire. Elle est par la suite invitée à composer un numéro de téléphone généralement surtaxé pour vérifier la situation de ce dernier. Ce numéro correspond à une boîte vocale, un message demande alors à la victime de fournir ses identifiants bancaires (les 16 chiffres et la date de validité de sa carte bancaire). Ces informations pourront ensuite être utilisées pour effectuer des achats frauduleux sur Internet.

Seconde méthode :

Une personne appelle une victime potentielle en se faisant passer pour quelqu'un du département de sécurité Visa, Master Card ou simplement de sa banque. Elle lui signale que sa carte de crédit a été utilisée pour un achat douteux et lui demande si elle est à l'origine de cette opération. Sa réponse étant négative, elle lui attribue un numéro de contrat de fraude, donnant ainsi à l'appel un aspect réaliste, puis lui demande de communiquer les coordonnées de sa carte bancaire afin de vérifier qu'elle est toujours en sa possession. Une fois la conversation terminée, la personne ajoute : n'hésitez pas à nous rappeler si vous avez d'autres questions et raccroche.

Comment s'en protéger ?

Les fraudeurs jouent sur une vulnérabilité psychologique du consommateur en créant en lui un stress et un faux sentiment d'urgence lié à la possibilité d'avoir été fraudé.

Si un message vous demande de rappeler tel numéro, ne le composez pas. Prenez le temps de retrouver le véritable numéro de téléphone qui vous a été donné par l'émetteur de votre carte de crédit et utilisez le.

Comme nous vous l'avons déjà dit, il faut savoir qu'aucune banque ne vous demandera par courrier électronique, télécopie ou téléphone ce genre de renseignements. Dans le doute, contactez votre établissement bancaire dans les plus brefs délais. Ne donnez jamais votre code confidentiel.

Pour les mairies, n'hésitez pas à communiquer cette information via internet et/ou bulletin municipal.

Soyez assurés Mesdames et Messieurs, de notre engagement entier et dévoué.

Adjudant-chef Christophe AUGUSTE
Référent Sûreté en prévention situationnelle et en vidéoprotection
Groupement de gendarmerie de la Drôme
Avenue Dupré de Loire – 26000 VALENCE
Tél : 04.75.82.56.66 / 06.24.62.38.36
christophe.auguste@gendarmerie.interieur.gouv.fr
referent-surete-ggd26@gendarmerie.interieur.gouv.fr